View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by B-Digital

Conceitos básicos e introdução ao tema da Gestão da Segurança da Informação no contexto do digital e dos Sistemas e Tecnologias de Informação

Gestão da Segurança da Informação

Luís Borges Gouveia

Versão 1.1 – Março de 2016

Gestão da Segurança da Informação

Conceitos básicos e introdução ao tema

Texto de conceitos em Sistemas e Tecnologias de Informação

Luís Borges Gouveia
Agregação em Engenharia e Gestão Industrial (UA)
PhD em Ciências da Computação (ULancaster)
MSc em Engenharia e Electrónica e de Computadores (FEUP)

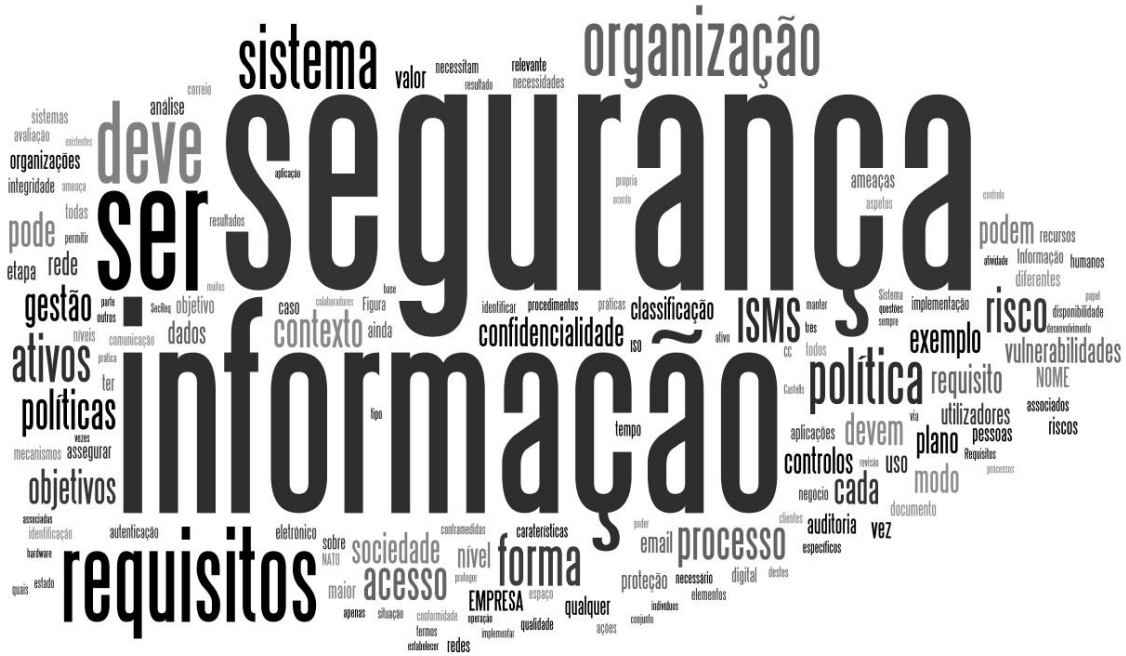
História do documento

V1.1 Adição de mais conteúdo e pequenas correções
V1.0 Edição e primeira versão pública para módulo de 10h em Segurança da Informação
V0.5 Criação e organização de conteúdos. Fevereiro de 2016.

Referências principais

Andress, Jason (2011). The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress. Elsevier.
ISO, *International Standards Organization* (2013). ISO/IEC 27001: 2013. *Information technology - Security techniques* - Information security management systems – requirements. Informação disponível em http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534, consultado a 14 de Março de 2016.

Nuvem de palavras do texto



Sobre o texto

No contexto atual, onde o uso de dispositivos e meios digitais é crescente, a importância de gerir a informação, torna-se mais crítica. Nesse contexto, um dos seus aspetos é a segurança da informação que é também sujeita a maiores desafios.

O texto propõe uma apresentação dos conceitos associados com a gestão e a identificação dos problemas associados com a segurança da informação e o esforço a realizar para, da melhor forma, lidar com vulnerabilidades e integrar a gestão da segurança da informação nas práticas associadas com a gestão da informação.

Objetivos do texto

1. Sensibilizar para a importância da segurança da informação nas organizações e introduzir os principais contextos associados
2. Introduzir o uso de métodos de avaliação do risco para suporte de uma auditoria de segurança da informação e para realizar sugestões de melhoria (recomendações)
3. Introduzir a avaliação de forma crítica, das ameaças e das vulnerabilidades à segurança da informação e sugerir potenciais modelos de soluções
4. Introduzir como conduzir uma auditoria de segurança da informação
5. Introduzir a avaliação crítica e a elaboração de um relatório de políticas de segurança da informação

Tabela de Conteúdos

Índice de figuras

Introdução à Segurança da Informação

A sociedade em rede e a complexidade do mundo que nos rodeia

Esta seção é um ensaio sobre a complexidade do ambiente que nos rodeia e que afeta necessariamente as necessidades de segurança da informação. Tem por base os trabalhos editados por Castells e Cardoso (2005), sobre o tema da sociedade em rede.

A sociedade em rede e as novas dinâmicas que emergem por efeito das transformações causadas pelo digital e pelo desenvolvimento de novas formas de relacionamento humano, colocam enormes desafios à forma como lidamos com a informação e o valor que esta tem para nós.

O conceito de sociedade em rede contempla um leque alargado de fenómenos que tem ocorrido a partir da segunda metade do século XX e à escala global. Trata-se do sucessor da pós industrialização, da sociedade da informação, do pós Fordismo, da pós-modernidade e/ou globalização, enquanto discursos que confluem para a prevalência da rede, em substituição da hierarquia como modo de organização mais comum, na forma como seres humanos interagem em sociedade.

Adicionalmente ao papel das redes, o crescente uso do digital e da mediação de tecnologias que o proporcionam (tecnologias de informação e comunicação) e que constituem a infraestrutura básica que serve de mediação quase que exclusiva, a um leque alargado de práticas sociais, políticas e económicas.

Segundo a formulação de Castells de 1998, a sociedade em rede é formada por redes de produção, poder e experiência, construindo uma cultura de virtualização nos fluxos globais que transcende o tempo e o espaço. Em conformidade, as instituições, pilares da sociedade, necessitam de se reorganizar de forma a dar resposta à extensão dos conceitos de tempo e espaço, de acordo com o digital que torna estes conceitos mais elásticos e os transforma e multiplica em diversas modalidades, muitas delas ainda em evolução.

Conforme Castells defendeu em 1998, numa sociedade em rede, o poder e a falta de poder são função do acesso a redes e do controle dos seus fluxos (recursos, informacionais e financeiros – que constituem ativos globais sensíveis e geralmente denominados *global commons*). Segundo o mesmo autor, as redes constituem-se como portas de acesso onde se sucedem oportunidades sendo que, fora das redes, a sobrevivência é cada vez mais difícil.

Castells propôs em 1996 o espírito do informacionalismo enquanto ética fundadora da empresa em rede (aliás, Castells sempre se recusou ao uso do termo Sociedade da Informação e preferiu em alternativa o termo, sociedade informacional).

O designado espirito do informacionalismo é resultado de muitas culturas e projetos, produto dos diversos intervenientes nas redes que a informam e são influenciados por ela, resultando em transformações organizacionais e culturais aceleradas. Esta dinâmica consegue constituir uma força material na medida em que informa, força e molda as decisões económicas e até estratégicas da (vida) da rede, sendo que este espírito constitui a forma de destruição criativa acelerada por via dos dispositivos eletrónicos e do digital.

Considerando a sociedade em rede e as questões da passagem do conhecimento às políticas a instituir, Castells (cap 1) defende que as transformações na nossa sociedade que ocorrem em modo crescentemente acelerado e iniciadas por volta de 1970 são despoletas pelo uso de computadores, mas claramente multidimensionais e resultado do molde que os indivíduos geraram da interação com computadores, redes e o digital.

Mas o mesmo Castells reforça o óbvio: que a tecnologia, embora necessária não é suficiente para a nova e emergente organização em rede que carateriza o número crescente de instituições e empresas com maior sucesso, influência e capacidade de sobrevivência num mundo em transformação. As tecnologias digitais têm possibilitado às redes, o ultrapassar dos seus limites históricos e com isso criar ruturas na forma como os seres humanos fazem a sua própria história e se organizam em sociedade.

Estas transformações são discutidas e passam pela economia, organização do trabalho, socialização e consciência do próprio indivíduo, até ao modo como comunicamos, organizamos os nossos sistemas políticos e representamos a nossa identidade coletiva, com impacte na noção de Estado. Tal tem necessariamente que ter implicações no modo como vivemos em sociedade e como nos regulamos, pelo que novas políticas devem ser desenvolvidas para o efeito, reformando em especial o setor público, pois é o que apresenta pela sua própria construção, maior inércia para as mudanças necessárias (não esquecendo a escola, a nossa noção de progresso, justiça, em especial que proteção legal e a quê – das patentes, ideias e produtos à propriedade privada).

Conclui, apresentando dois dos dilemas do nosso tempo: (1) criatividade e libertação pelo conhecimento ou capitalismo 2.0; e (2) democracia participativa ou controle político. Por sua vez, Cardoso (cap 2) alerta que a Internet como tecnologia pode ser objeto de apropriação e utilização de forma conservadora, sem tal significar mudanças significativas de hábitos e práticas em uso na sociedade.

Por outras palavras, a hipótese de a Internet se constituir como a ferramenta de desenvolvimento e construção de projetos tem de ser tomada com prudência, uma vez que pode ser utilizada apenas como mais uma ferramenta disponível e alternativa, reduzindo o seu uso à repetição de práticas existentes. Não obstante, a Internet potencia e ajuda as práticas de transição em Portugal (vista como uma

sociedade em transição) para a sociedade em rede (considerada como processo que se encontra em curso, mas com caraterísticas próprias de outros países desenvolvidos ou em desenvolvimento). Não obstante, importa salientar que a realidade observada a nível global, europeu e nacional, entre os dados observados da primeira década do novo milénio são diversos e relativos a uma situação que evoluiu rapidamente e carece de nova reflexão e atualização.

Jorgwnasen e Khuong (cap 3) e Soete (cap. 4) discutem questões associadas com o fator trabalho e as implicações deste fator para o emprego, a produtividade, o valor acrescentado e a inovação. Estas questões da economia em rede confrontam com os fenómenos sociais da globalização e as forças geradas por estas dinâmicas, que tem do mundo ocidental uma resposta coletiva por via da sociedade da informação e um constante esforço pelo equilíbrio do desenvolvimento sustentável nas suas dimensões social, económica e ambiental ou de recursos.

Adicionalmente é também realizada a discussão das diferentes perceções sobre estes desafios em função de modelos económicos e culturais macro, como é o caso dos EUA e da Europa (embora atualmente existem em confrontação outros blocos que a globalização trouxe para atores principais, nomeadamente os BRICs – uma designação conjunta para Brasil, Rússia, India e China).

No que se refere à reforma organizacional são considerados diferentes áreas como o papel dos Estados, a questão da Saúde e do bem-estar social, a questão da educação e da aprendizagem (e já agora, da criação, partilha e difusão de conhecimento) e as questões de contexto legal associadas com a atividade económica. Estes capítulos apresentam um conjunto de elementos que contribuem para a reflexão e concretização do que é entendido por sociedade em rede.

No que se às políticas de transição para a sociedade em rede (parte VI) são apresentadas as perspetivas políticas no seu sentido mais nobre de encontrar caminhos e do assumir da decisão política como opção consciente no sentido de levar a efeito um espaço de transição sem tumulto e disrupção (que poderia inviabilizar o essencial de uma transição de valor e sustentada) para a sociedade em rede.

A emergência de novas formas de comunicação social e socializada: transitando dos meios de comunicação em massa para os meios de auto comunicação em massa proporcionam uma escala de tempo e espaço nova: mais imediato e mais próximo.

Muito mediado pelo digital e com recurso a meios tecnológicos sofisticados, é auto gerado em conteúdo e auto direcionado em emissão e ainda auto selecionado na receção, num ambiente em que muitos comunicam com muitos, proporcionando um sistema dinâmico, altamente volátil e difícil de prever e de enorme dificuldade de rastrear.

Consideramos a comunicação digital como um novo espaço público da sociedade em rede e que, de momento, recorre à Internet e a redes sociais, mas que pode e vai evoluir para formas não facilmente identificáveis de momento.

Neste contexto, o ciberespaço é o "local" de convergência de fluxos de informação que expressam as relações de poder enquanto novo espaço de comunicação, sendo em consequência um espaço de conflito e de poder numa sociedade mais digital e global – como tal, necessariamente objeto de atenção e de concentração de meios de segurança e defesa pelas entidades que pretendam deter o poder efetivo.

Segurança da Informação

Segurança da Informação

A informação é utilizada pelas organizações, independentemente sejam lucrativas ou não. A informação satisfaz as necessidades de informação de modo a permitir o reconhecimento das caraterísticas de um determinado contexto e suportar a decisão, com vista a garantir uma ação de acordo com os objetivos pretendidos e com a realidade envolvente (ação informada).

As organizações empresariais também necessitam de informação e esta pode ser entendida como um ativo de grande valor que é materializado e em muitos formatos distintos. Nem todos são digitais, como o papel, mas muitos dos formatos são, cada vez mais digitais. Exemplos de informação em suporte digital é a que existe em registos de computador, em bases de dados e noutras das inúmeras aplicações com que as empresas suportam o seu dia-a-dia.

Gerir toda esta informação de um modo eficaz, tornou-se essencial para o futuro do negócio em causa. Em consequência, a segurança da informação (enquanto ativos de potencialmente grande valor) não deve mais ser visto como uma atividade menor, no contexto das organizações – mesmo daquelas que não sendo empresariais, também possuem informação crítica, como é o caso das organizações estatais, de administração pública, ou mesmo do governo. A proteção destes ativos de valor, associados com a informação é designada por segurança da informação.

A segurança da informação é a proteção de informação, dos sistemas e dos dispositivos (hardware) que usa, armazena e transmite informação. O objetivo da segurança da informação é o de proteger de forma adequada os ativos de informação de modo a assegurar a continuidade de negócio (ou de operação, se for preferido o uso de um termo menos associado à vida empresarial), minimizando potenciais perdas que possam ocorrer (da perda ou destruição de valor desses ativos) e maximizando o retorno de investimento (uma vez que os esforços associados com a proteção de informação tem de ser cobertos pelo seu valor ou pelo valor que deles se possa extrair). Para atingir este objetivo, é necessário preservar três aspetos críticos da informação, que são: a confidencialidade, a integridade e a disponibilidade.

A apresentação correta destes aspetos da informação garante a credibilidade e confiança nas organizações e nos negócios e pode ser alcançada, com base na aplicação de controlos. Os controlos podem ser mais ou menos sofisticados e são resultado de uma combinação de políticas, procedimentos, estruturas organizacionais e mecanismos de medida física ou de *hardware* e *software*.

De um modo geral, a segurança da informação é um requisite obrigatório, de forma a minimizar os riscos associados a uma atividade ou negócio e assegurar

a conformidade com disposições legais ou de natureza regulatória, como é o caso de regulamentos comunitários ou provenientes da legislação nacional.

Caraterísticas da Informação

O valor da informação é resultado das próprias caraterísticas que a informação possui. Se, por qualquer motivo, a informação altera alguma das suas caraterísticas, o valor da informação também é alterado. Normalmente, essa alteração resulta numa diminuição de valor. Por exemplo, o exato momento em que a informação se encontra disponível é um fator crítico para os utilizadores, porque, muitas vezes, a informação perde todo o seu valor, quando não é entregue em tempo. Mesmo que os profissionais de segurança da informação e os utilizadores finais partilhem o mesmo entendimento das caraterísticas da informação, cada um destes grupos dá a estas caraterísticas, diferentes prioridades – a que podem corresponder diferentes sistemas de proteção.

Existem três aspetos associados com a informação que são bastante utilizados na prática, como referenciais, quando se procura garantir a segurança da informação. Esses aspetos são confidencialidade; integridade e disponibilidade.

Confidencialidade

A confidencialidade da informação é a qualidade ou estado de prevenir exposição ou acesso não autorizado à informação, por parte de indivíduos ou sistemas. A confidencialidade da informação (em Inglês, *confidentiality*) deve assegurar que apenas aqueles que possuem direitos e privilégios de acesso a um particular conjunto de informação é que são capazes de o fazer. Este acesso legal é muitas vezes referido por acesso autorizado e é permitido a entidades credenciadas para o efeito.

A proteção de confidencialidade deve prevenir que aqueles que não devem ter acesso à informação, não o possam ganhar, por qualquer forma possível ou alternativa. Quando indivíduos ou sistemas não autorizados puderam ganhar acesso à informação, estamos perante uma falha do sistema e pode ser afirmado que houve um comprometimento ou falha de confidencialidade.
Um exemplo de quebras de confidencialidade são as mediáticas fugas de informação do segredo de justiça.

Integridade

A integridade da informação é a qualidade ou estado da informação em que esta constitui um todo e se encontra completa e não corrompida. O termo em Inglês é *integrity*. Por exemplo, quando um dos seus componentes sobre uma alteração ou eliminação não detetável. Existe sempre a ameaça à integridade da informação, quando ela está exposta a modificação não autorizada, ou a corrução ou mesmo a danificação ou outra qualquer forma de disrupção do seu estado de

autenticidade. A ameaça de integridade pode ocorrer quando esta esta a ser armazenada ou transmitida.

Disponibilidade

A disponibilidade da informação significa que a informação está acessível a sistemas e utilizadores autorizados, sem qualquer interferência ou obstrução e de modo a ser devidamente percebida, isto é, no formato requerido. O termo em Inglês é *availability*. A disponibilidade de informação assegura que apenas os utilizadores que foram verificados como tendo a autorização adequada (credenciais) para a informação é que lhes é concedido o acesso, sempre e quando o pretendam – no tempo e no espaço, ou a qualquer momento e em qualquer lugar – disponibilidade total (por vezes, a referência a altos níveis de disponibilidade requeridos é referida como alta disponibilidade e é uma das caraterísticas dos sistemas críticos).

Análise de risco em segurança da informação

Uma vez que não é possível garantir uma proteção total à informação a todas as ameaças (conhecidas e não conhecidas), torna-se necessário conduzir uma análise de risco da segurança da informação, de modo a determinar as ameaças e as vulnerabilidades para a informação e as contramedidas necessárias para serem aplicadas de modo a reduzir (mitigar) o efeito destes riscos (impacto) para um nível aceitável.

Desta forma, a análise de risco é um processo de identificar os ativos, os riscos para esses ativos e os procedimentos para mitigar os riscos para esses ativos. As organizações ou os indivíduos necessitam de entender quais os riscos que existem no seu ambiente de ativos de informação e como esses riscos podem ser reduzidos ou mesmo eliminados. A gestão do risco é o processo de implementar e manter as contramedidas que reduzem os efeitos do risco para um nível aceitável.

É da análise de risco que a informação que é necessária para a gestão tomar decisões acertadas relativas à segurança da informação de uma organização, é obtida. Essa obtenção por esta via, devesse ao facto da análise de risco identificar os controlos de segurança no local, calcular as suas vulnerabilidades e avaliar o efeito das ameaças, em cada área ou situação de vulnerabilidade

A gestão do risco deve ser um processo em curso, proativo, de modo a estabelecer e manter um nível aceitável de segurança de um sistema de informação. Uma vez alcançado um nível adequado de segurança, o processo de gestão de risco monitoriza o risco nas atividades quotidianas (ou correntes) e segue os resultados da análise de risco de segurança.

Os passos associados com a condução de uma análise de risco são:

1. Identificar e estimar o valor dos ativos: os primeiros passos na avaliação de risco são identificar e atribuir um valor ao ativos que necessitam de ser protegidos. Exemplo de ativos nestas condições podem ser *software*, *hardware*, mesmo recursos humanos e fontes de informação. Um exemplo de informação pode ser um ficheiro de clientes ou um processo de produção que seja sensível para a organização, ou ainda, como no caso da justiça, informação sobre um processo em segredo de justiça;

2. Identificar ameaças associadas com os ativos: as ameaças são eventos ou condições que podem ainda não ter ocorrido mas que podem potencialmente ocorrer e que a sua presença provoca um aumento de risco. Depois de identificar os ativos que necessitam de proteção, a ameaça a estes ativos deve ser identificada e examinada para determinar as suas consequências (impacto). Por exemplo, um ataque por vírus, uma quebra de segurança por um *hacker*, entre uma enorme multiplicidade de possibilidades;

3. Identificar as vulnerabilidades: as vulnerabilidades são situações ou condições que aumentam a ameaça o que, por sua vez, aumenta o risco. Assim, as vulnerabilidades que aumentam o risco, devem ser identificadas;

4. Determinar as contramedidas necessárias: é o processo de eliminar, erradicar ou mitigar a ameaça e assim anular o risco. Determinar as contramedidas para reduzir a ameaça leva a ações como a instalação de *firewalls,* em redes de computador na esperança de gerir o risco associado com os acessos indevidos. Um ativo possui uma certa quantidade de risco que lhe é inerente e está associada com a ameaça. A vulnerabilidade apenas torna o risco maior e as contramedidas servem para diminuir o risco. O risco residual é o que é deixado existir, depois das contramedidas serem aplicadas – o risco em boa verdade numa é totalmente nulo.

Controlos de segurança da informação

Os controlos de segurança da informação são contramedidas de gestão, ou operacionais, ou ainda técnicas, recomendadas para os sistemas de informação, para proteger a confidencialidade, integridade e disponibilidade de um sistema e da sua informação. Os controlos de segurança, quando utilizados de forma adequada, podem prevenir, limitar ou deter uma ameaça aos ativos de uma organização.

Os controlos de segurança podem ser divididos em métodos técnicos métodos não técnicos.

Os controlos técnicos são contramedidas que são concebidos no contexto dos computadores: *hardware*, *software* e *firmware*. Exemplos deste tipo de controlos são os mecanismos de controlo de acesso, os mecanismos de identificação e autenticação, métodos de encriptamento e de deteção de intrusões; todos eles desenvolvidos com recurso a programas de computador e implementados em dispositivos eletrónicos (*hardware*); como aplicações (*software*) ou embebidos em dispositivos específicos como processadores (*firmware*).

Quer os controlos controlos técnicos, quer os controlos não técnicos, podem ser divididos em preventivos ou de deteção:

- Controlos de prevenção são os controlos que impedem ou desencorajam as tentativas de violar as políticas de segurança. Por exemplo, controlos de acesso e de condicionamento de acesso, encriptação e autenticação;

- Controlos de deteção notificam ou informam da violação ou tentativa de violação de uma política de segurança. Por exemplo, sistemas de auditoria; métodos de deteção de intrusões; ou somas de verificação (*checksums*);

O contexto é muito importante e o conhecimento da situação existente crucial. Por exemplo, é muito importante saber que a implementação destes controlos para mitigação do risco, dependem da qualidade dos controlos que existem já no contexto dos ativos a proteger. Se um desses controlos tiver alguma deficiência (que crie uma ou mais vulnerabilidades) ou se determinado controlo não existir ou estiver desativado, o próprio processo de avaliação do risco sai distorcido ou com deficiências de leitura da avaliação da situação real.

Classificação da informação

Tipos de informação de acordo com a sua confidencialidade

No contexto da Sociedade da Informação e da crescente importância da informação, importa salvaguardar o seu uso e proteger dados e informação de modo a preservar o seu valor.

Deste modo, as preocupações com a segurança são importantes e a norma ISO 27000 constitui a principal família de normas para a segurança da informação, em que é apresentada a classificação de informação de acordo com a sua confidencialidade e a norma está apoiada nos princípios da integridade, disponibilidade e confidencialidade da informação

Processo de classificação de informação

O processo de classificação de informação, possui quatro etapas. Para a operacionalização destas quatro etapas é desenvolvida uma política de classificação da informação. As etapas a considerar são:

1. Identificar a informação como um ativo a inventariar
2. Classificação da informação
3. Rotulagem da informação
4. Manipulação e manuseio da informação

A primeira etapa é identificar a informação como um ativo a inventariar. O objetivo do esforço de desenvolvimento de um inventário de ativos é para obter uma lista exaustiva de quais os itens de informação que devem ser classificados e quem é responsável por cada um deles (o seu dono).

A informação classificada pode estar em diferentes formatos e tipos de media, como por exemplo:

- Documentos eletrónicos
- Sistemas de informação / bases de dados
- Documentos em papel
- Meios de armazenamento (discos, usb, etc.)
- Informação transmitida verbalmente
- Correio eletrónico (*email*)

A segunda etapa, é a classificação da informação, propriamente dita. A norma ISO 27001 não prescreve os níveis de classificação, mas permite a liberdade de adotar o que é mais comum no país ou setor da indústria.

Assim, quanto maior e mais complexa a organização, mais níveis de confidencialidade terá. Por exemplo, para organizações de média dimensão, podem ser considerados 4 níveis de classificação da informação, com três níveis de confidencialidade e um nível público, conforme apresentado a seguir.

Níveis de classificação de informação:

- Confidencial (o mais alto nível de confidencialidade)
- Restrita (médio nível de confidencialidade)
- Uso interno (o mais baixo nível de confidencialidade)
- Pública (todos podem ver a informação)

Em muitos casos, o dono do ativo é o responsável por classificar a informação, o que é feito com base nos resultados da análise/avaliação de riscos. Quanto maior o valor da informação (amplifica as consequências de uma quebra da confidencialidade), maior deverá ser o nível de classificação.

É frequente uma organização dois ou mais esquemas de classificação diferentes implementados. Em geral, os níveis de classificação estão também relacionados com os contextos de uso e exploração de informação que tem de ser considerados na organização. Por exemplo, no caso de trabalhar tanto como o setor governamental, quanto com o privado.

Um exemplo é a NATO, que classifica a informação em seis níveis, com quatro níveis de confidencialidade restrita e dois níveis públicos:

- Altamente secreto (*Cosmic Top Secret*)
- NATO Secreto (*NATO Secret*)
- NATO Confidencial (*NATO Confidential*)
- NATO Restrito (*NATO Restricted*)
- NATO Não Classificado (direito autoral) (*NATO Unclassified (copyright)*)
- Informação não sensível, de domínio público (*Non sensitive information releasable to the public*)

A terceira etapa é a rotulagem da informação. Uma vez classificada a informação, é necessário a sua rotulagem. Neste contexto, devem ser desenvolvidas orientações para cada tipo de ativo de informação sobre como ele precisa ser rotulado. Mais uma vez, a norma ISO 27001 não prescreve soluções fixas, pelo que estas devem ser desenvolvidas com recurso a regras próprias (o que pode constituir uma vantagem, ao permitir uma maior adaptação ao contexto da organização).

Por exemplo, a definição de regras de rotulagem da informação, para documentos em papel de forma que:

- O nível de confidencialidade seja indicado no canto superior direito de cada página do documento;
- A classificação da informação seja indicada na capa ou no envelope que transporta o documento (e protege a sua manipulação direta);
- Também deve ser colocada a classificação na pasta onde o documento é armazenado.

A rotulagem da informação é geralmente da responsabilidade do proprietário da informação

Por último, a quarta etapa diz respeito à manipulação e manuseio de ativos. Trata-se da parte mais complexa do processo de classificação. Consiste no desenvolvimento de regras sobre como proteger cada tipo de ativo, dependendo do seu nível de confidencialidade. Neste contexto deve ser organizada uma tabela com a listagem de ativos e o seu nível de confidencialidade, que incluía também, as medidas de segurança associadas.

Um exemplo é definir que um documento em papel, classificado como restrito, que deve ser guardado em espaço próprio (cofre/armário fechado). Outro exemplo é, que documentos podem ser transferidos dentro e fora da organização, apenas em envelope fechado e no caso de ser enviado para fora da organização, o documento deve ser enviado com registo ou em mão própria, com registo prévio dos ativos manipulados

Neste contexto, da manipulação e manuseio de ativos, a norma ISO 27001 permite definir as regras próprias da organização. Estas são geralmente definidas na política de classificação da informação ou nos procedimentos de classificação.

O processo de classificação pode ser complexo, mas tem de ser claro e facilmente aplicável, de forma a poder ser seguido e controlado. Também neste contexto, a norma ISO 27001 dá uma grande liberdade, permitindo adaptar um processo a necessidades especiais, de forma a assegurar que a informação sensível esteja protegida.

Planeamento de segurança

Plano de segurança

Um plano de segurança é um documento estruturado que descreve como uma organização irá abordar todas as suas necessidades de segurança. O plano é subjetivo e varia de um contexto organizacional para outro contexto, pois cada organização é distinta das demais, ainda mais se a considerarmos como um sistema que organiza atividade humana e, portanto, dependente dos recursos humanos específicos de cada organização, da sua história e competências.

O plano de segurança é um documento dinâmico e que acompanha a evolução da própria organização, pelo que precisa de revisto e melhorado, de forma periódica. A alteração do plano de segurança depende essencialmente das necessidades da organização, das suas necessidades de segurança e dos resultados da gestão de risco. Um bom plano de segurança é um registo oficial da prática de segurança corrente, na organização.

Conteúdos de um plano de segurança

Os conteúdos do plano de segurança devem incluir tanto uma descrição do estado de segurança atual, como os planos de melhoria futura, para a organização. As organizações podem ter ou não, especialistas para desenvolver um processo de planeamento de segurança formalmente definido ou recorrer a consultores externos para este fim. Cada plano deve ter em consideração os seguintes sete aspetos:

1. Política de segurança
2. Situação actual
3. Requisitos
4. Controlos recomendados
5. Responsabilidade (*accountability*)
6. Calendário
7. Rotina de revisão do plano

1. Política de segurança

Uma política de segurança é uma declaração de alto nível de propósito e de intenção de uma organização em relação à segurança da informação. As políticas devem incluir as linhas orientadoras para uma intenção específica para todas as pessoas, em todos os níveis da organização (envolver a totalidade dos recursos humanos é um fator chave para uma correta política de segurança).

A produção de uma política de segurança da informação não é uma tarefa muito difícil, mas a sua implementação revela-se mais complexa. As normas de segurança proporcionam a orientação para conseguir obter políticas de

segurança específicas, muitas vezes adaptadas a produtos ou tecnologias bem determinadas e particulares. O que é importante é que seja fornecida uma direção da política bem precisa e clara e que a gestão de suporte para a sua implementação permita a concretização da segurança da informação e da sua correta manutenção.

Para ser efetiva, a política deve ser relevante, acessível e facilmente entendível pelos potenciais utilizadores na organização. A política necessita de empenho da gestão, ao mais alto nível, para suporte dos seus procedimentos, a disponibilização de um enquadramento técnico adequado que permita a sua implementação e a afetação de um grau apropriado de autoridade, pela qual, a conformidade com a política possa ser verificada e com respostas legais que permitam responder de forma eficaz às suas violações.

Por vezes, as organizações disponibilizam um outro documento designado por procedimento ou diretrizes (guião) para definir como uma política se traduz em ações concretas.

Uma declaração de política deve responder a três questões essenciais:

- A quem deve ser autorizado o acesso à informação?
- A qual sistema e recursos da organização é que o acesso deve ser autorizado?
- Qual o tipo de acesso que deve ser atribuído a cada utilizador e para cada recurso?

Uma declaração de política deve cobrir os seguintes tópicos:

- Âmbito e meta em matéria de segurança
- As obrigações legais e regulamentares
- Funções e responsabilidade para a segurança
- Abordagem estratégica e princípios da organização que esta gostaria de seguir

Ação no caso de violação da política (quebra de política)

Por outro lado, uma boa política de segurança deve possuir as seguintes caraterísticas:

- Cobertura: uma política de segurança deve ser abrangente, ser aplicada de forma explícita a todas as situações possíveis (que já existam ou ainda desconhecidas) na organização. Uma política de segurança não deve ser atualizada sempre que uma nova situação possa ocorrer;

- Reduzir a ambiguidade e assegurar a utilidade: as terminologias utilizadas para formular a política devem ser claras, completes e usadas com precisão para a construção da política de segurança. Desta forma, a política de segurança deve ser escrita numa linguagem que seja compreendida por todos. A política deve ser realística para ser

implementada na infraestrutura existente. Adicionalmente, deve ser aplicável com vantagens em termos de custo, tempo e conveniência;

- Durabilidade: uma política de segurança deve crescer e ser adaptável, de forma a sobreviver ao crescimento de um Sistema e à sua expansão, sem sofrer mudanças. As políticas devem também muda devido a mudanças na regulamentação, novas ou alterações de necessidades dos clientes e em outros casos de influência exterior à própria organização;

- Suporte da gestão e alta direção: deve ser obtido o apoio e o empenho da gestão e alta direção da organização, sempre que possível. Esse apoio deve ser dado de forma inequívoca;

- Papeis e responsabilidades: todos os papeis e responsabilidades devem ter o consenso de todas as partes implicadas e cm responsabilidade.

Estrutura do conteúdo do documento de uma política de segurança

Uma política de segurança deve identificar a sua audiência. Dessa forma, os beneficiários, os utilizadores e os donos da política e a própria política devem todos eles estar expressos de forma clara e direta. Por sua vez, a política de segurança deve ter em conta a natureza da sua audiência e dos seus objetivos de segurança, pelo que não existem políticas de segurança universais – estas devem ter em consideração, o contexto concreto do ambiente de pessoas, tecnologia e organização (o sistema de informação) em que são aplicadas.

Propósito

A política deve enunciar o propósito das funções de segurança da organização, refletindo os requisitos dos beneficiários, dos utilizadores e dos donos. Os objetivos devem ser considerados de áreas diversas, tais como:

- Proteger de forma eficiente a operação de negócio;
- Facilitar a partilha de informação;
- Salvaguardar a informação pessoal e de negócio;
- Assegurar uma informação precisa;
- Assegurar um ambiente de trabalho seguro e produtivo;
- Assegurar a conformidade com a lei e as regulamentações me vigor.

Recursos protegidos

Os ativos críticos necessitam de ser protegidos. Estes ativos devem ser listados na política de segurança.

Natureza da proteção

A lista de ativos indica o que deve ser protegido. Uma política de informação deve também indicar quem deve ter acesso às peças de informação protegidas, como o acesso será realizado, como serão autorizadas pessoas em particular (credenciação) e como será negado o acesso às restantes. A política de segurança deve indicar o grau de proteção que será proporcionado a cada ativo ou, pelo menos, a cada tipo de recursos.

Políticas em gestão da segurança da informação

As políticas mais associadas com as tecnologias de informação e comunicação mudam mais rapidamente do que as políticas de empresa. Como são detalhadas, necessitam de ser revistas de forma mais regular. Exemplos de políticas específicas são:

- Classificação de informação;
- Recuperação de incidentes (*disaster recover*);
- Controlo de acessos;
- Operações;
- Gestão de incidentes;
- Cópias de segurança (*backup*);
- Segurança física;
- Chaves criptográficas;
- Acesso de terceiros e convidados;
- Segurança da Internet;
- Gestão de continuidade de negócio.

À medida que as organizações crescem e se tornam mais complexas, com mais colaboradores e maior volume de informação a tratar, processar, comunicar e armazenar, os métodos existentes para comunicação tendem a ser menos eficazes. Se apenas se tornarem lentos, trata-se de um problema de eficiência, com impacto na qualidade da operação. Mas por vezes, causam mesmo rupturas e levam a falhas de comunicação ou outras que afetam a própria operação, neste caso, constituindo um problema ainda de maior gravidade, associado com a eficácia.

O crescimento das organizações torna assim menos eficazes entendimentos informais e negociações ou conversas de corredor, como forma de partilhar informar e acertar práticas. Por outro lado, também as pressões legais e de

regulamentos aumentam, com a expansão das organizações. Torna-se assim necessário providenciar que toda a organização seja coberta com uma governação clara, concisa e que possa trazer benefícios reais de eficiência e ao mesmo tempo, de redução do risco associado à informação (mau uso). Neste contexto, uma política de segurança da informação pode reduzir a ambiguidade; providenciar um rumo claro de gestão e um comprometimento dos responsáveis; e o estabelecimento de papéis e responsabilidade previamente acordados.

Considerar estes aspetos, pode proporcionar os meios para lidar com as dificuldades que são inevitáveis e que resultam da necessidade de gerir informação. Estas dificuldades podem incluir um balanceamento entre a necessidade de partilhar informação e a necessidade de restringir o seu acesso. Uma política é uma expressão de intenção. Necessita de ser suportada por políticas subordinadas (específicas) e por procedimentos pragmáticos (adaptados à realidade do contexto de aplicação). Um mapa geral de políticas e da forma como se relacionam é apresentada na Figura 1.

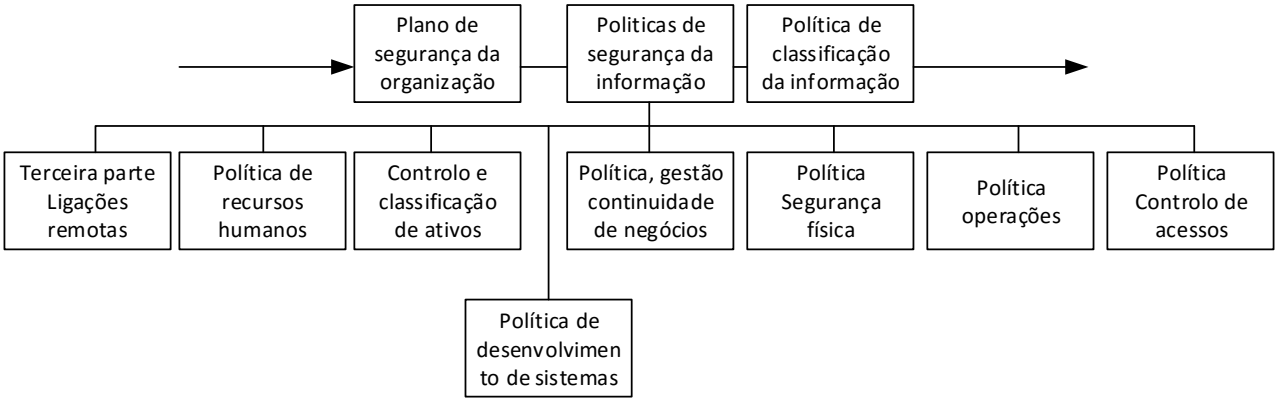


Figura 1: Estrutura de políticas subordinadas para a segurança da informação (adaptado de BERR, 2004

No contexto atual, a segurança da informação é ainda um maior desafio, em resultado do incremento dos dispositivos moveis e da sua capacidade de capturar informação, mesmo do mundo não digital e de a disseminar de forma rápida e fácil, por via do digital. Exemplos são o uso do correio eletrónico e das redes sociais que permitem a partilha rápida e muitas vezes, despreocupada e sem cuidado, de informação relevante e mesmo até sensível, para uma organização.

Neste contexto, um número crescente de organizações estão a criar as suas próprias políticas de segurança da informação para ordenar o uso deste tipo de serviços. Um dos primeiros e mais essenciais é o correio eletrónico. A *Figura 2* apresenta um exemplo da estrutura de uma política de segurança da informação para o uso de correio eletrónico.

Política de correio eletrónico (email)

1.0 Propósito (objetivo)
Prevenir uma vulnerabilidade da imagem pública da <NOME DA EMPRESA>, quando um email é enviado da <NOME DA EMPRESA> para outros destinos. O público em geral tende para considerer a mensagem enviada como uma afirmação oficial da <NOME DA EMPRESA>.

2.0 Abrangência
Esta política cobre o uso apropriado de qualquer mensagem de correio eletrónico enviada dos endereços de email da <NOME DA EMPRESA> para todas os *stakeholders* tais como colaboradores, vendedores e agentes, operando em nome da <NOME DA EMPRESA>.

3.0 Política de correio eletrónico da <NOME DA EMPRESA>

3.1 Uso proibido. O Sistema de email da <NOME DA EMPRESA> não deve ser utilizado para qualquer uso pessoal ou para a criação ou distribuição de mensagens disruptivas ou ofensivas, incluindo comentários ofensivos sobre raça, género, cor do cabelo, deficiências, idade, orientação sexual, pornografia, crenças e práticas religiosas, posições políticas ou associadas com a nacionalidade de pessoas. Os colaboradores que recebem qualquer email do exterior que abranja um ou mais dos aspetos descritos, deve reportar de forma imediata a situação ao seu superior hierárquico.

3.2 Uso pessoal
A utilização de uma quantidade razoável de recursos da <NOME DA EMPRESA> para envio de emails pessoais é aceitável. Mas o email relacionado com aspetos que não sejam de trabalho deve ser guardado numa área diferente do email relacionado com o trabalho. O envio de cadeias de email ou cartas, ou emails com piadas e outras mensagens do mesmo teor, do email da <NOME DA EMPRESA>, é proibido.

3.3 Monitorização
Os colaboradores da <NOME DA EMPRESA> não devem ter expetativas de privacidade em qualquer coisa que armazenam, enviem ou recebam no sistema de correio eletrónico da <NOME DA EMPRESA>. Por seu lado a <NOME DA EMPRESA> pode monitorizar as mensagens sem notificação prévia. A <NOME DA EMPRESA, no entanto, não é obrigada a manter um serviço de monitorização às mensagens de correio eletrónico.

4.0 Execução
Qualquer colaborador que tenha violado esta política pode ser sujeito a um processo disciplinar, que pode incluir mesmo a cessação do seu contrato de trabalho.

5.0 Definições

Termo	**Definição**
Correio eletrónico (email)	A transmissão eletrónica de informação através de um protocolo como o SMTP, o IMAP ou o Webmail. Os clientes típicos de email incluiem o Eudora e o Microsoft Outlook ou um navegador, como o Chrome, o Edge, o Safari ou o Firefox.
Email encaminhado	Um email reenviado de uma rede interna para um ponto exterior.
Cadeia de email ou carta	Um email enviado a sucessivas pessoas. Tipicamente, o corpo do email contém informação associada a marcas, pedidos, notícias de interesse de um grupo alargado de pessoas ou ainda sugere benefícios ou penalizações caso se quebre a cadeia de envios.
Informação sensível	Informação considerada sensível e que pode ser nociva, caso divulgada para a <NOME DA EMPRESA> ou coloca em causa a reputação da marca no mercado ou mesmo dos clientes.
Divulgação não autorizada	Revelação intencional ou não intencional de informação restrita a pessoas, tanto dentro como fora da <NOME DA EMPRESA>, que não tem necessidade de ter acesso a essa informação.

6.0 História do documento
Lista de versões, com número, data e pequena descrição

Figura 2: Exemplo de uma política de segurança da informação para o correio eletrónico (adaptado de SANS)

2. Situação atual

Para ser capaz de planear para a segurança, uma organização deve entender quais as vulnerabilidades a que está exposta. As vulnerabilidades podem ser determinadas por via da realização de uma análise de risco, investindo numa investigação cuidadosa do Sistema, do seu ambiente e de tudo o que poderá correr mal nele.

Os resultados da gestão de risco formam a base para a descrição do estado atual da segurança. Em particular, permite o reporte dos ativos, das vulnerabilidades e ameaças, de quais são os ativos críticos e os mecanismos de proteção.

O estado de segurança reportado, também define os limites da responsabilidade para a segurança. Não só define quais os ativos que necessitam de ser protegidos mas também quem é o responsável pela proteção desses ativos.

3. Requisitos

Os requisites são as restrições relacionadas com os objetivos de segurança. Os requisitos de segurança constituem o núcleo da segurança na elaboração de qualquer plano de segurança. Ao contrário dos típicos requisitos de sistema ou requisitos funcionais, os requisitos de segurança podem ser potencialmente reutilizados, num domínio ou contexto semelhante, especialmente se especificados como instâncias de modelos reutilizáveis.

Os requisitos de segurança são desenvolvidos para especificar as políticas de segurança do sistema e ambas políticas como requisitos devem mapear os riscos de segurança já identificados, as ameaças e as vulnerabilidades. Os requisitos devem também suportar a implementação de um plano de segurança.

Os mecanismos de segurança (tais como identificação de utilizadores, senhas de acesso «*passwords*», criptografia, *firewalls* e *software* antivírus) são então pensados para satisfazer os requisitos de segurança- Alguns destes conceitos, influenciam a engenharia associada com os requisitos de segurança (isto é, políticas, riscos, ameaças e ativos), enquanto outros (isto é, mecanismos de segurança, vulnerabilidades e ataques) são influenciados pelos requisitos de segurança.

A figura 3, apresenta os relacionamentos entre alguns dos conceito mais relevantes, descritos no âmbito da segurança da informação. Com base na figura, é possível considerar que a base são os ativos. Os ativos podem ser um ou mais e de três tipos diferentes: humanos (pessoas); propriedade (coisas) e serviços (operações). Nos ativos que se constituem por coisas, designadas coletivamente como propriedade, podem ser de quatro tipos diferentes: dados, *hardware*, software e infraestruturas.

Como já referido, os ativos permitem sobre eles, a existência de ameaças e vulnerabilidades. As vulnerabilidades exploram as ameaças existentes e proporcionam os ataques que resultam em riscos de segurança, tal como as próprias ameaças. A existência de mecanismos de segurança, por sua vez, permitem reduzir as vulnerabilidades e suportam os requisitos de segurança. São os requisitos de segurança que especificam as políticas de segurança´, que por sua vez, estabelecem os objetivos de segurança – a Figura 3 resume todas estas relações, de um modo gráfico, mostrando também os termos em língua Inglesa.

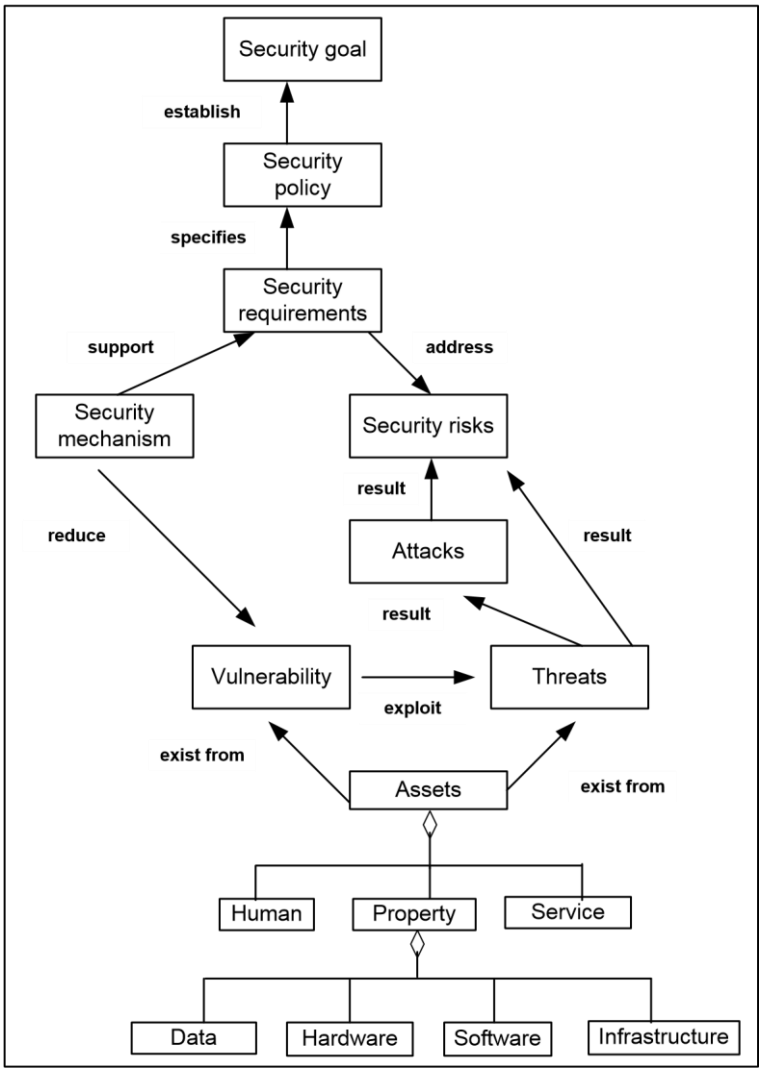


Figura 3: Conceitos de segurança e os seus relacionamentos

4. Controlos recomendados

Os controlos recomendados são mapeados e associados com as vulnerabilidades identificadas na política e nos requisitos. Os requisitos de segurança demonstram as necessidades de sistema em termos do que deve ser protegido. O plano de segurança deve também recomendar quais os controlos que devem ser incorporados no sistema para satisfazer os requisitos especificados.

Os controlos recomendados abordam as questões de implementação: como os sistemas podem ser concebidos e desenvolvidos para dar resposta aos requisitos de segurança especificados.

5. Responsabilidade pela implementação

Nesta parte deve ser especificado quais as pessoas que são responsáveis por implementar os requisitos de segurança. Esta documentação suporta quem tem a tarefa de coordenar as responsabilidades individuais em conjunto com os especialistas em segurança. Ao mesmo tempo, o plano torna explícito quem é (ou pode ser) responsável, se existem requisites que não possam ser cumpridos e vulnerabilidades a que não foi dada resposta.

Existem muitos e diversos papéis na organização a considerar, tais como a conceção, o desenvolvimento, a utilização e a manutenção do sistema. Tal leva a diferentes perfis de recursos humanos envolvidos diretamente no sistema, tais como utilizadores finais, gestores de projeto, gestores, administradores de bases de dados, administrativos, entre muitos outros. Quando a dimensão da organização é relevante (por exemplo mais de 30 colaboradores), deve existir uma equipa de planeamento de segurança que realiza uma análise de segurança e recomenda um programa de segurança. Deve ainda ser responsável pela sua escrita e pela atribuição de responsabilidades a pessoas específicas na organização, para a execução de tarefas. A equipa pode ser constituída por 5 a 9 elementos em função da dimensão da organização. No entanto, é também possível que uma pessoa apenas possa dar suporte a todas as tarefas, numa organização mais pequena.

6. Calendário

Um plano de execução do uso de tempo e que seja compreensivo, é sempre necessário. No entanto, é sempre difícil de executar, considerando o contexto real de uma organização. Mas o objetivo deve ser assegurar o controlo dos riscos com maior prioridade de vigilância, logo que possível, implementando as ações de controlo apropriadas.

O plano de segurança inclui um plano de tempo que mostra como e quando os elementos do plano são realizados. Estas datas também fornecem os marcos a atingir que servem de referência para que a gestão possa acompanhar o progresso da sua implementação.

7. Rotina de revisão do plano

A monitorização do plano, certamente desempenha um papel importante para qualquer sistema de gestão de segurança da informação. É necessário garantir que o sistema é tão seguro como é suposto que seja. Desta forma, para avaliar as soluções de segurança, as práticas de segurança e as políticas de segurança em

operação, quer o plano, quer os requisitos de segurança são importantes, agindo como referenciais para todo o processo.

O plano de segurança deve ser revisto, de forma periódica. Existem alguns outros fatores como a evolução da tecnologia, a mudança de vulnerabilidades e de ataques, a obsolescência das soluções, a alteração do quadro legal ou regulamentário e procura dos clientes, que exigem a revisão do sistema de gestão de segurança da informação existente de uma organização.

Medir os requisitos de segurança da informação

Um requisito de segurança é um requisito que qualifica, especificando, uma dada quantidade (sentimento) de segurança. De facto, como dimensão da segurança, o sentimento de segurança denomina a sensação de existência de segurança e induz a confiança de que se está perante um sistema seguro, logo confiável.

Um requisito também pode ser definido em termos de um critério específico de sistema e um nível mínimo de uma medida de qualidade associada que é necessário para satisfazer uma ou mais políticas de segurança. No entanto, existem desafios na captura e descrição e análise dos requisitos de segurança. Alguns destes desafios são:

- Os requisitos de segurança pode ser implícitos, escondidos ou espalhados por diferentes partes de especificações de requisitos, principalmente em texto;
- Qualquer erro num Sistema pode levar a uma falha de segurança;
- Torna-se monótona e bastante sujeita a erros, a procura manual num documento ou a avaliação de requisitos durante a sua recolha;
- Os recursos são normalmente limitados para suporte da análise de segurança;
- Existem documentos que compilam requisitos e podem constituir uma ajuda, como é o caso das normas ISO 14508 (*Common Criteria*, CC) e ISO 17799. No entanto, são documentos estáticos e que não tem em linha de conta ameaças que sejam novas ou emergentes;
- Os requisitos de segurança necessitam de ser não ambíguos e bem específicos, de modo a assegurar que os princípios de segurança e conceção segura sejam bem empregues;
- Na fase de recolha de requisites, deve ser devidamente detetadas as situações em que se está perante pedidos não documentados ou vagos, ou mesmo desejos de múltiplos *stakeholders*. Estas situações devem ser avaliadas e consideradas com cautela e ponderação nos requisitos documentados.

Podemos definir os requisitos de segurança como:

- Requisito de segurança: (i) Uma qualidade ou requisito que descreve que uma parte de um sistema deve ser seguro, ou (ii) uma propriedade que, se violada, pode ameaçar a segurança do sistema.
- Requisito relevante de segurança: (i) Um requisito que deve ser definido (está presente) num ou mais requisitos de segurança, ou (ii) uma propriedade que é potencialmente importante para avaliar a segurança de um sistema. Exemplo: o operador do cartão que usou um dispositivo POS (*point of sale*) para uma transação, utiliza o mesmo dispositivo que foi

usado para a compra, para realizar o cancelamento, em caso de necessidade.

Processo de levantamento de requisitos SecReq

O processo SecReq desenvolve um conjunto de critérios comuns, baseados no levantamento de requisitos de segurança com recurso a uma metodologia de rastreamento. O objetivo do SecReq é para ajudar em todas as etapas do levantamento de requisitos de segurança e fornecer mecanismos para rastrear os requisitos de segurança de objetivos de segurança de alto nível para a conceção de um sistema seguro. O SecReq combina três técnicas distintas que foram integrados para atender a essa meta:

- Uso do padrão CC (*common criteria*), do seu processo de levantamento de requisitos de segurança e do seu processo de refinamento;
- A ferramenta HeRA com as suas regras heurísticas, relacionadas com a segurança;
- Os estereótipos UMLsec, que oferecem uma conceção segura para o sistema.

O processo de levantamento de requisitos SecReq é composto por seis passos:

Passo 1: Especificar os objetivos de segurança a partir dos objetivos do sistema e dos requisitos funcionais

- Esta etapa envolve derivar os objetivos de segurança dos objetivos do sistema e dos seus requisitos funcionais. Outras fontes para os objetivos de segurança são a arquitetura de sistemas e a arquitetura da informação, descrições de conceito, ou qualquer outro sistema de informação relevante disponível, tais como as normas existentes. As classes funcionais de segurança CC, podem oferecer orientação ao longo desta etapa. A HeRA suporta este refinamento através da identificação de requisitos de segurança relevantes e pela realização das perguntas certas para o refinamento.

Passo 2: Associar uma classe funcional de segurança para cada um dos objetivos de segurança

- Durante este passo, para cada objetivo de segurança, a classe de requisito funcional de segurança relevante é selecionada a partir do CC. Mais uma vez, a HeRA pode sugerir uma classe funcional de segurança adequada com base em heurísticas.

Passo 3: Refinar os objetivos de segurança para objetivos de segurança de maior detalhe

- A tarefa desta etapa é a de refinar cada objetivo de segurança em um ou mais objetivos de segurança com maior detalhe. Cada destes sub-objetivos deve cumprir uma ou mais das famílias CC, contidos dentro da classe funcional relevante da etapa anterior. A ferramenta da HeRA também é utilizada para auxiliar nesta etapa, identificando os objetivos adicionais de segurança candidatos e orientando o processo de refinamento.

Passo 4: Refinar os objetivos de segurança mais detalhados para elaborar os requisitos de segurança

- Esta etapa envolve refinar cada objetivo segurança detalhado em um ou mais requisitos de segurança apoiados pelos componentes contidos da família CC, *common criteria* relevante (ou seja, a família utilizada para o objetivo de segurança detalhado). A ferramenta HeRA também é usada para auxiliar este passo, bastante semelhante à etapa 3.

Passo 5: Limitar os requisitos de segurança a requisitos de segurança específicos

- Esta é a última etapa da parte de exigência de levantamento do processo SecReq e refina cada requisito de segurança em um ou mais requisitos específicos de segurança, suportados pelos elementos contidos nos componentes CC relevantes (ou seja, os componentes utilizados para os requisitos de segurança). Como na etapa 3 e 4, a ferramenta HeRA suporta esta etapa, identificando potenciais requisitos de segurança adicionais. Mais uma vez, ele orienta o processo de refinamento com um assistente interativo.

Passo 6: Analisar os requisitos de segurança usando o UMLsec

- Esta é a parte de análise do processo SecReq. O objetivo deste passo é verificar se a conceção de segurança contém os requisitos de segurança específicos obrigatórios, desejados e opcionais que foram levantados. Esta análise inclui a verificação dos modelos UML que especificam o projeto, para cumprimento das exigências e que viabiliza o rastreamento da solução concebida, através dos requisitos de segurança específicos, de acordo com os objetivos de segurança. Esta análise exige que todos os requisitos de segurança sejam desencadeados nos passos 1 a 5 ao nível de abstração dos elementos funcionais de segurança CC (requisitos de segurança específicos).

Os requisitos de segurança da informação

Como enunciar as necessidades de garantia em termos de segurança da informação, nas organizações? A forma correta é através da especificação de um

conjunto de requisitos que expressa como se deve lidar com as diferentes preocupações que cada contexto específico levanta, em função das suas vulnerabilidades, das ameaças existentes e do risco que elas representam. A Figura 4 apresenta seis grandes grupos de requisitos de segurança da informação, sendo que três delas ainda possuem uma sub divisão (controlo de acessos, integridade e privacidade).

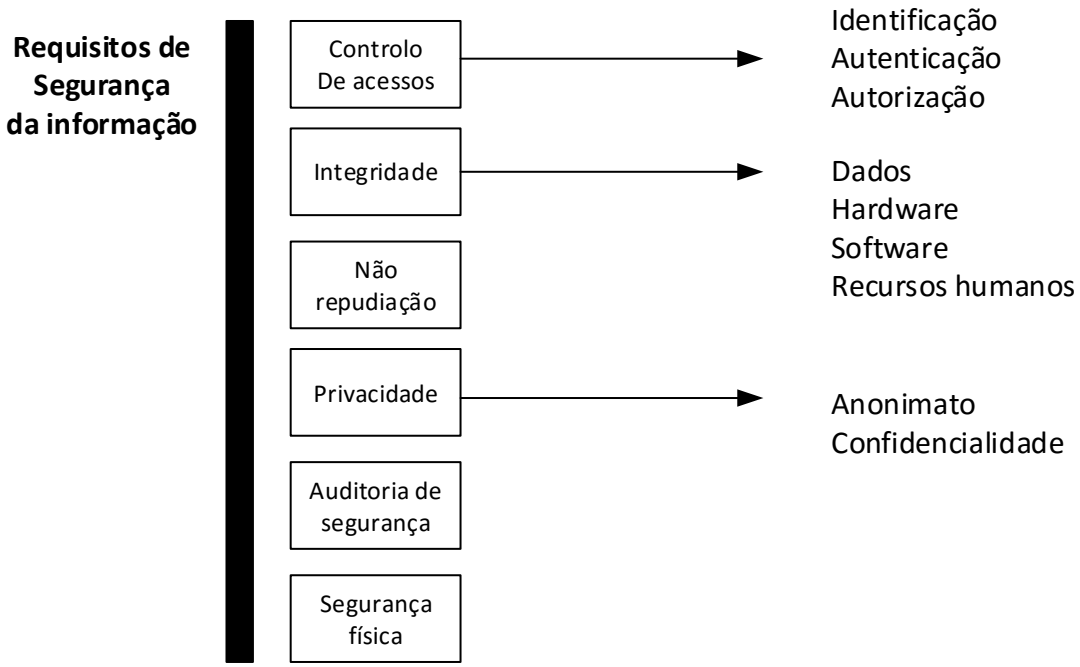


Figura 4: Grandes grupos dos requisitos de segurança da informação

Baseado na estrutura de organização dos requisitos da Figura 4, os diferentes grupos de requisitos de segurança da informação são apresentados.

Controlo de acessos, que incluem três subtipos: identificação, autenticação e autorização:

- Requisitos de identificação: um requisito de identificação que especifica até onde um sistema deve identificar os seus utilizadores (que podem ser seres humanos e aplicações externas), antes mesmo de interagir com eles. Os requisitos de identificação são tipicamente insuficientes por si mesmos, mas constituem um pré requisito para os requisitos de autenticação. Exemplo de um requisito de identificação: um sistema deve identificar todos os seus utilizadores antes de permitir o seu acesso ao sistema.
- Requisitos de autenticação: um requisito de autenticação verifica a identidade dos utilizadores (seres humanos e aplicações externas) antes de interagir com elas. Assim, os objetivos típicos de um requisito de autenticação são assegurar que os elementos externos são verdadeiramente quem são ou o que são (ou afirmam ser) e dessa forma

evitar comprometer a segurança devido a um impostor. A autenticação depende da identificação, Se a identidade é importante especificar, também o é, a autenticação. Um exemplo de um requisito de autenticação é: um sistema deve verificar a identidade de todos os seus utilizadores antes de lhes permitir atualizar a sua informação de utilizador.

- Requisitos de autorização: um requisito de autorização lida com o acesso e os privilégios de utilização de utilizadores autenticados. O requisito assegura que os utilizadores autenticados tenham acesso a aplicações ou dados específicos, com um nível previamente acordado. A autorização pode ser concedida a pessoas individuais ou a aplicações ou a grupos de pessoas relacionadas ou a grupos de aplicações. Um exemplo de um requisito de autorização é: o sistema não deve permitir o acesso dos agentes de serviço de clientes, à informação dos cartões de crédito dos clientes.

Os requisitos de integridade que incluem os requisitos que confirmam que uma aplicação ou componente deva assegurar que os seus dados e comunicações não são intencionalmente corrompidos por via da criação, modificação ou eliminação não autorizadas. Os objetivos típicos de um requisito de integridade são os de assegurar que comunicações e dados são de confiança. Um exemplo de um requisito de integridade é: o sistema deve prevenir situações não autorizadas de alteração (corrupção) de dados recolhidos dos clientes e outros utilizadores externos.

- Os requisitos de deteção de intrusão especificam que uma aplicação ou componente deve detetar e registar as tentativas de acesso ou modificação realizadas por indivíduos não autorizados. O objetivo principal é detetar indivíduos não autorizados e programas que tentam aceder a uma aplicação ou componente e registar informação sobre as tentativas de acesso não autorizado de acesso e notificar os eventos (incidentes) em conformidade. Um exemplo de um requisito de deteção é: o sistema deve notificar qualquer tentativa de acesso falhada de forma repetida, no acesso a bases de dados.

Os requisitos de não repudiação confirmam as ações de um utilizador e previnem que negue as suas interações com partes do sistema ou dentro do próprio sistema (por exemplo, mensagens ou transações). Estes requisitos asseguram que os registos de atividade adequados são mantidos (para permitir a rastreabilidade de cada ação e utilizador). Em resultado, uma significativa quantidade de informação deve ser armazenada como resultado de cada interação.

Os requisitos de privacidade consideram que o negócio, as aplicações, os componentes ou as bases de dados, devem manter os seus dados sensíveis e as comunicações de forma privada, protegidas do acesso não autorizado de indivíduos e aplicações. Os requisitos de privacidade estão relacionados mas vão além dos requisitos, porque as pessoas e aplicações devem ter acesso apenas a

dados e aplicações para os quais estejam autorizadas. Os requisitos de privacidade necessitam de estar alinhados com restrições legais como as leis que exigem que certos dados (por exemplo, informação de cartões de crédito) tenha de ser mantida privada – leis de proteção de dados. É assim necessário assegurar que sejam especificados acessos não autorizados e a informação seja classificada.

Requisitos de auditoria de segurança. Uma auditoria de segurança lida com as capacidades de um sistema suportar audições de estado e uso dos seus mecanismos de segurança. Assegura que uma aplicação ou componente recolhe, analisa e reporta informação sobre o estado dos seus mecanismos e das suas utilizações. As atividades de auditoria (*audit trails*) e os registos de eventos (*logs*) são importantes para este contexto.

Requisitos de proteção física. Este tipo de requisitos proporciona uma restrição que uma aplicação ou centro de dados deve se proteger a si própria de um assalto físico. Em particular, um sistema deve ser protegido de danos físicos, destruição, roubo ou substituição de *hardware*, alteração de *software* ou pessoal devido a vandalismo, sabotagem ou terrorismo. Este tipo de requisitos está também relacionado com requisitos de sobrevivência ou de resiliência.

Sistema de Gestão de Segurança da Informação

A organização internacional de normalização (ISO – *International Organization for Standardization*) providencia um modo para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um Sistema de gestão de segurança da informação (ISMS – *Information Security Management System*).

Um ISMS constitui uma opção estratégica de uma organização em que é adotada uma abordagem estruturada para a segurança da informação, orientada aos processos, que permite estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um ISMS.

As áreas de atuação de um ISMS são:

- Identificar e analisar os requisites de segurança da informação e a necessidade de estabelecer uma política e objetivos para a segurança da informação;
- Uma prática estruturada de gestão do risco no contexto da organização e dos riscos de negócio, associados à organização;
- Supervisionar e rever o desempenho e eficácia de um ISMS;
- Melhoria contínua baseada na medida e avaliação de objetivos.

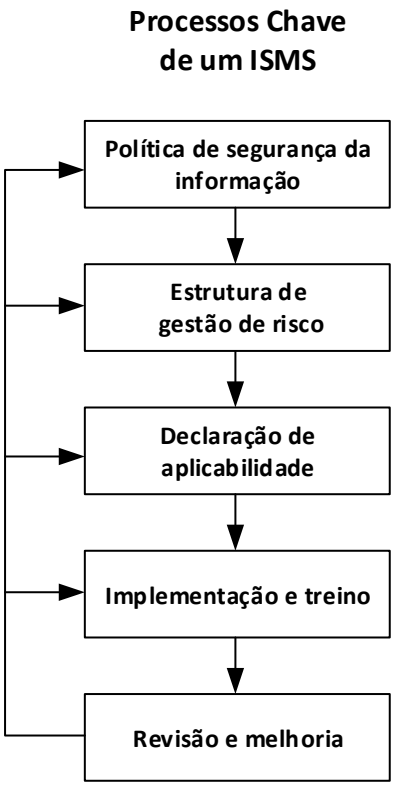


Figura 5: Processos chave de um ISMS (ISO 27001)

A Figura 5 esquematiza os cinco processos chave que devem ser considerados num sistema ISMS. A sequência desses processos chave tem de permitir a revisão e retorno a cada um dos processos de modo a assegurar a adaptação do sistema ISMS à organização e às solicitações do seu meio envolvente, numa lógica de melhoria contínua.

Considerar o ciclo PDCA – uma caraterística do recurso a normas ISO – segue um esquema como o apresentado na Figura 6. Para um ISMS siga uma abordagem do ciclo PDCA, deve ser considerado o seguinte, para cada uma das fases do ciclo:

- Planear (*plan*) – definir o ISMS: estabelecer as políticas do ISMS. Os seus objetivos, processos e procedimentos relevantes para a gestão do risco e melhoria da segurança da informação de modo a garantir os resultados adequados para a organização e para os seus objetivos e políticas;
- Fazer (*do*) – executar o ISMS: implementar e operar as políticas, controlos, processos e procedimentos de um ISMS;
- Verificar (*check*) – monitorizar o ISMS: avaliar e, quando aplicável, medir o desempenho de processos das políticas, objetivos e experiência prática de um ISMS e reportar os resultados à gestão, para revisão;
- Agir (*act*) – manter e melhorar o ISMS: realizar ações corretivas e preventivas, baseadas nos resultados de auditorias internas ao ISMS e à gestão de revisão e outra informação relevante, de modo a conseguir uma prática de melhoria contínua do ISMS.

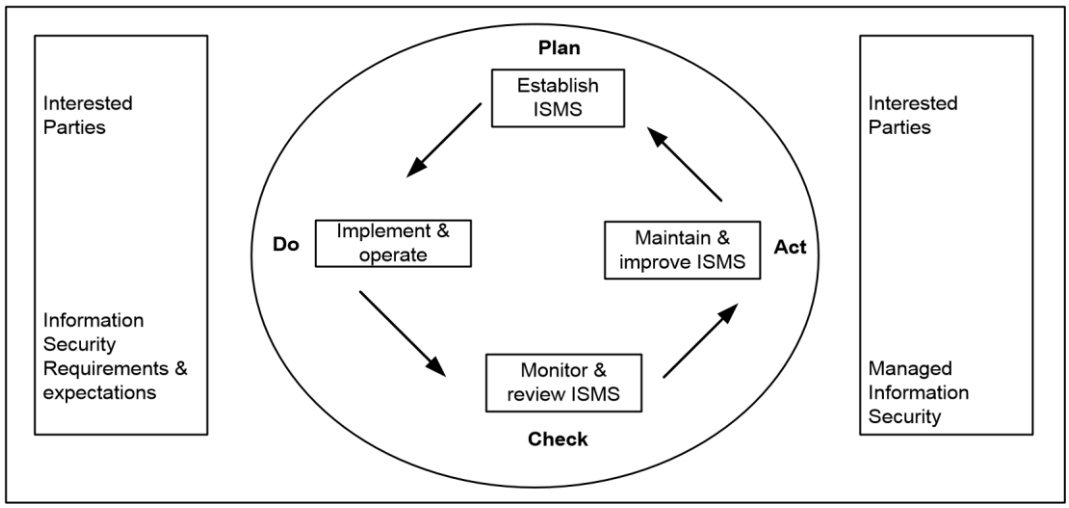


Figura 6: Ciclo PDCA, como base do modelo ISMS

Requisitos gerais de um ISMS

Baseado no ciclo PDCA, é necessário considerar as seguintes atividade para viabilizar um ISMS. Na prática, os quatro momentos associados com a adoção de um ciclo PDCA para um sistema ISMS, leva a (i) estabelecer e gerir um ISMS;

(ii) implementar e operar um ISMS; (iii) monitorizar e rever a operação de um ISMS; e (iv) manter e melhorar um sistema ISMS.

1. Estabelecer e gerir um ISMS:
   - Para estabelecer um ISMS, deve ser definido um contexto de forma clara, com uma abrangência e as fronteiras do sistema, relacionadas em particular definindo as caraterísticas do negócio, a estrutura da organização, os seus objetivos, a sua localização, os seus ativos e as necessidades de tecnologia. A abrangência também inclui detalhes e justificação de todas as exceções a considerar no contexto da abrangência;
   - Definir uma política para um ISMS em termos das caraterísticas do negócio, da organização, da sua localização, ativos e tecnologia de modo a permitir uma orientação clara da direção da informação;
   - Uma prática abrangente da gestão de risco.

2. Implementar e operar um ISMS:
   - Conduzir uma gestão de rico e implementar ações de controlo de riscos;
   - Gerir recursos;
   - Treinar os colaboradores.

3. Monitorizar e rever a operação de um ISMS:
   - Executar, monitorizar e rever políticas e procedimentos;
   - Identificar tentativas e quebras de segurança existentes;
   - Ações a tomar para eventuais quebras de segurança;
   - Manutenção de eficácia das práticas de segurança existentes;
   - Revisão regular;
   - Medir a eficácia das ações de controlo;
   - Rever a avaliação de risco.

4. Manter e melhorar um sistema ISMS:
   - Melhorar um ISMS;
   - Ações preventivas e corretivas;
   - Comunicar as ações e melhorias a todas as partes interessadas.

Auditoria a um sistema ISMS

As auditorias são utilizadas para determinar até que ponto, os requisites do Sistema de gestão da qualidade d segurança da informação, são satisfeitos. Os resultados da auditoria são utilizados para avaliar a eficácia do Sistema de gestão da qualidade e para identificar as oportunidades de melhoria.

Uma auditoria é um processo sistemático, independente e documentado para obter evidências e elementos de avaliação de forma objetiva, para determinar até que ponto é que cada critério de auditoria é satisfeito.

Termos utilizados em contexto de auditoria

Existe um conjunto de termos associados com a atividade de auditoria e que definem os elementos e práticas associadas. Alguns dos termos mais relevantes são:

- *Critérios de auditoria*: um conjunto de políticas, procedimentos ou requisitos;
- *Evidência de auditoria*: registos, afirmações de factos ou outra informação relevante, para os critérios de auditoria e para os resultados verificáveis da auditoria da avaliação das evidências recolhidas de acordo com os critérios de auditoria estabelecidos;
- *Conformidade*: satisfação de um requisito;
- *Não conformidade*: Não satisfação de um requisito;
- *Defeito*: não satisfação de um requisito, relacionada com um uso específico ou intencional;
- *Ação preventiva*: Acão para eliminar a causa de uma potencial não conformidade ou outra situação potencial, não desejável;
- *Ação corretiva*: Acão para eliminar a causa de uma não conformidade detetada ou outra situação não desejável.

Processo de certificação

O processo de certificação com vista ao estabelecimento e manutenção de um sistema de gestão de segurança de informação com qualidade e fiável é obtido por via de um processo de certificação que se inicia com um processo de quatro passos. O primeiro passo está associado com questões de implementação e contempla um estudo prévio de como pode na organização ser implementado um sistema associado com a segurança da informação. Em resultado, esse estudo deve ser objeto de avaliação e em função do estudo de implementação e da avaliação realizada, o terceiro passo é proceder à auditoria para a partir daí, lhe dar seguimento (quarto passo) com ações de revisão e melhoria contínuas.

Em todo o processo, deve existir uma consciencialização para a segurança da informação, pelos colaboradores e alta direção da organização.

Por sua, vez, os elementos humanos diretamente envolvidos no processo de certificação devem estar comprometidos de um modo forma, por via de um acordo de salvaguarda de confidencialidade, de forma a proteger a informação e o conhecimento das vulnerabilidades e demais aspetos associados com a segurança da informação da organização. O objetivo de todo o processo é naturalmente, a obtenção de uma certificação ISMS, do seu sistema de gestão de segurança da informação. O esquema do processo de certificação está esquematizado na Figura 7.

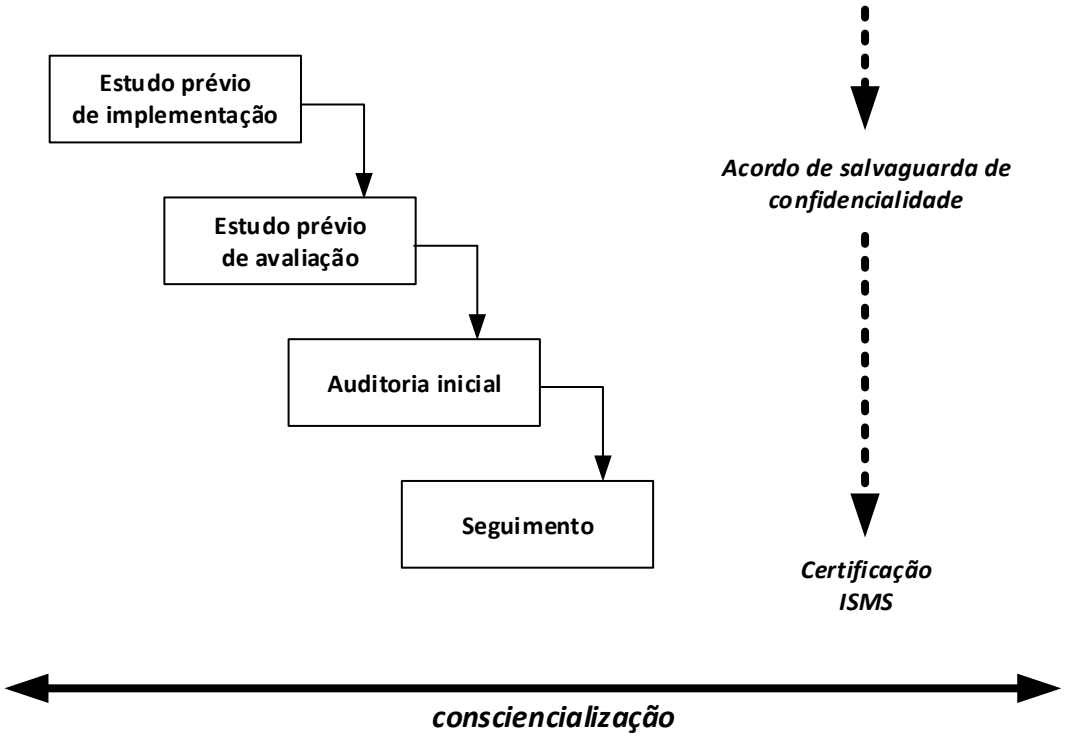


Figura 7: O processo de certificação

Exemplo de um lista de verificação para auditor um ISMS

A realização de uma auditoria deve produzir documentação que seja simples e objetiva. De um modo estruturado e sintético, devem ser objeto de reporte, o essencial dos resultados obtidos. Neste contexto, o quadro seguinte, apresenta uma possível estrutura para a auditoria e uma lista de verificação para o esforço a realizar.

- Nome do auditor:
- Data:
- Equipa de auditoria:
- Organização:
- Contato na organização:
- Contexto:
- Sistemas de informação:
- Serviços:

Lista de verificação de auditoria Gestão de segurança da informação (ISO 27001)						
Referência		**Área de auditoria, objetivo e questão**			**Resultados**	
Lista de verificação		**Norma**	**Seção**	**Questão de auditoria**	**Descobertas**	**Conformidade**
Política de segurança						
A.5	5.1	Política de segurança da informação				
		Documento da política de segurança da informação	Verificar: - Se existe uma política d segurança da informação - Se a política foi aprovada pela direção - Se a política foi publicada e comunicada de forma apropriada para todos os colaboradores			
Organização da segurança da informação						
A.6	6.2	Organização interna				
		Compromisso da gestão com a segurança da informação	Verificar se existe uma estrutura de gestão que assegura que existe uma orientação clara e um suporte efetivo da direção, para as iniciativas de segurança, dentro da organização			

Gestão de ativos					
7.1	1	Responsabilidade sobre os ativos			
		Inventário dos ativos	Verificar que o inventário ou registo é mantido contendo os ativos importantes para cada sistema de informação Verificar para cada ativo identificado, se tem dono, qual a classificação de informação correspondente e a sua localização e caraterísticas		
7.1	3	Uso aceitável dos ativos	Verificar se estão definidos os procedimentos apropriados para um uso aceitável dos ativos		
Controlo de acessos					
A11	1.1	Políticas de controlo de acesso	Verificar se os requisitos de negócio para o controlo de acessos foram identificados e documentados Verificar se a política de controlo de acessos está de acordo com as regras e os direitos de cada utilizador ou perfil		
Gestão de acesso dos utilizadores					
	9.2	Registo de utilizadores	Verificar se existe um registo formal de utilizadores e um procedimento descontinuação de registo, que engloba a atribuição/retirada de direitos de acesso a múltiplos serviços e sistemas de informação		

Exemplo de um relatório de auditoria em segurança da informação

Relatório de auditoria

É o sumário de um exercício de auditoria, normalmente baseado em listas de verificação e na investigação das instalações da organização. Não existe um formato bem definido para um relatório de auditoria, mas dele devem constar alguns tópicos. Entre estes, devem existir os seguintes:

Sumário executivo
A auditoria foi realizada para rever o sistema de gestão de segurança da informação da <NOME DA ORGANIZAÇÃO>. A auditoria é baseada na norma ISO 27001 e a que organização da <NOME DA ORGANIZAÇÃO> deve estar conforme e respeitar a norma.

Um conjunto de preocupações relevantes foram identificadas, N no total, na falha de procedimentos sob as políticas relacionadas com o sistema de gestão de segurança da informação. Uma recomendação de alta prioridade foi enunciada, relacionada com as deficiências detetadas na adesão às seguintes políticas: política de controlo de acessos e política de recursos humanos, conforme é especificado nos anexos A, B, C, …

Enquadramento
Para cada exercício de auditoria, são identificados e verificados de forma rigorosamente verificados e avaliados de forma crítica, os controlos em ação para o sistema de gestão de segurança da informação. São identificadas as potenciais vulnerabilidades que se tornaram visíveis como resultado do exercício de auditoria. Foram também recolhidos um conjunto de comentários dos colaboradores envolvidos para cada uma das vulnerabilidades identificadas e questionada a gestão para fornecer planos de ação que detalham os cronogramas previsíveis para implementar as recomendações efetuadas.

Abrangência e objetivos
O contexto e objetivos da auditoria foram assegurar que a <NOME DA ORGANIZAÇÃO> segue as diretrizes da norma ISO 27001.

Abordagem da auditoria
A abordagem para o trabalho realizado tomou a seguinte estratégia:

- Discutir com os recursos humanos relevantes da organização e desenvolver um entendimento dos processos e procedimentos estabelecidos na <NOME DA ORGANIZAÇÃO>, para conseguir estar em conformidade com a norma ISSO 27001;

- Avaliar se os sistemas associados e os procedimentos, documentos, registos são apropriados para satisfazer os objetivos da <NOME DA ORGANIZAÇÃO> e do seu sistema de gestão da segurança da informação;
- Avaliar a consciência dos colaboradores para os seus papéis e responsabilidades para lidar com um sistema de gestão da segurança da informação;
- Determinar a efetividade e a eficácia das políticas de segurança

Conclusão
Com base no trabalho desenvolvido, a opinião defendida é que a <NOME DA ORGANIZAÇÃO> deve ter consideração o seguinte:

- <NOME DA ORGANIZAÇÃO> está **não conforme/conforme** com a norma ISO 27001;
- As políticas são **inadequadas/adequadas** para o cumprimento da norma ISSO 27001.

A revisão efetuada identificou um número de deficiências na adesão à norma, nas políticas e procedimentos seguidos, que os responsáveis da organização necessitam de considerar de forma a fortalecer o sistema de gestão da segurança da informação. Foram identificadas **N** situações, reportadas como objeto de recomendações de alta prioridade.

Recomendações de alta prioridade

Ref	Aspeto	Recomendações	Resposta da direção plano de ação
1	Seguir a recomendação A.5.1 As políticas de segurança da informação não são entendidas de forma clara, pelos colaboradores	Todos os colaboradores necessitam de treino apropriado É necessário implementar políticas	O treino de colaboradores será objeto de ações de formação em XXXX sobre os temas YYY e ZZZZ

Anexo A: Sumário detalhado dos resultados da auditoria

Ref	Observação da auditoria	Resposta da gestão
1	Não existe evidência que todas as políticas estejam disseminadas pela organização Não existe evidência de treino dos colaboradores	Foi reconhecido que as políticas não estão devidamente disseminadas e existem falhas no treino dos colaboradores para o ISMS Necessário ações de treino
2	Falta um processo de gestão de riscos Não existe registo sobre avaliação e gestão de riscos identificados	Foi reconhecido que não existe registo do desempenho da gestão de risco, mas existe um processo de gestão de riscos

Referências

BERR. (2004). *Information Security: How to Write an Information Security Policy*. Department for Business Enterprise & Regulatory Reform. UK.gov.

Castells, M. and Cardoso, G. (eds). (2005) *The Network Society: From Knowledge to Policy*. Centre for Transatlantic Relations: Johns Hopkins University. Disponível em *http://www.umass.edu/digitalcenter/research/pdfs/JF_NetworkSociety.pdf*, consultado em 4 de Março de 2014.

Gouveia, L. (2006). Negócio Electrónico: conceitos e perspectivas de desenvolvimento. Livro I – Colecção Negócio Electrónico. Dezembro de 2006. SPI – Principia.

Gouveia, L. (2011). Gestão das organizações, natureza, âmbito e complexidade. INA, Porto. Abril. *http://pt.slideshare.net/lmbg/gestodas-organizaes-natureza-mbitoe-complexidade*, consultado em 17 de Março de 2016.

Gouveia, L. (2014). Segurança Informática. Contexto, conceitos e desafios. Rotary Club Vizela. 18 de Junho. Disponível em *http://pt.slideshare.net/lmbg/segurana-informtica*, consultado em 17 de Março de 2016.

Gouveia, L. (2014). The Information Warfare – how it can affect us. Rethinking Warfare Conference. UFP, Porto. 10th November. Disponível em *http://pt.slideshare.net/lmbg/the-information-warfare-how-it-can-affect-us*, consultado em 17 de Março de 2016.

Gouveia, L. (2015). Conjunto de transparências do módulo de Segurança da Informação e Proteção de Dados. Formação em Direção da Segurança. CEFOC. Universidade Fernando Pessoa.

Gouveia, L. (2015). Informação digital e segurança. Ciclo de Conferências sobre Segurança e Cidadania – GNR. Lisboa. 11 de Março. Disponível em *http://pt.slideshare.net/lmbg/11mar-gnrlx2015*, consultado em 17 de Março de 2016.

Gouveia, L. (2015). O digital, a mobilidade e a economia da privacidade. Conferência Privacidade, Inovação e Internet. APDSI. Cultugest. Lisboa. 30 de Janeiro. Disponível em *http://pt.slideshare.net/lmbg/o-digital-a-mobilidade-e-a-economia-da-privacidade*, consultado em 17 de Março de 2016.

Gouveia, L. and Gaio, S. (eds) (2004). Readings in Information Society. University Fernando Pessoa Press. March.

Gouveia, L. e Gaio, S. (editores) (2004). Sociedade da Informação: balanço e implicações. Junho de 2004. Edições Universidade Fernando Pessoa.

Gouveia, L. e Ranito, J. (2004). Sistemas de Informação de Apoio à Decisão. Livro VII - Colecção Inovação e Governância nas autarquias. Dezembro de 2004. SPI – Principia.

SANS (s/d). *Repositório de materiais sobre Segurança da Informação e cibersegurança*. Disponível em *http://www.sans.org/security-resources/policies/*, consultado em 17 de Março de 2016.